Testovanie bezpečnosti – demo

1. MITRE ATT&CK je primárne zdrojom informácií o
   ☐ technikách a postupoch útočníkov
   ☐ technikách a postupoch detekcie útokov
   ☐ bezpečnostných opatreniach
   ☐ taktikách a postupoch pri red teamingu

2. Ktorý z uvedených nástrojov a služieb **nie je** použiteľný pre pasívny prieskum (Passive Reconnaissance)
   ☐ HaveIBeenPwned
   ☐ crt.sh
   ☐ Shodan
   ☐ Nessus

3. Vyhľadanie pdf dokumentov v doméne uniba.sk dosiahneme v Google nasledovne
   ☐ filetype:pdf site:uniba.sk
   ☐ fileext:pdf site:uniba.sk
   ☐ filetype:pdf intitle:uniba.sk
   ☐ fileext:pdf intitle:uniba.sk

4. ARP sken nám prezradí
   ☐ MAC adresy živých systémov
   ☐ IPv6 adresy živých systémov
   ☐ ARP adresy živých systémov
   ☐ žiadne z predchádzajúcich

5. SUID flag nastavený na spustiteľnom programe **nečakáme** pre
   ☐ `passwd`
   ☐ `base64`
   ☐ `sudo`
   ☐ `mount`

6. SSH local port forwarding (`ssh -L 1234:webserver:443 user@sshserver`) bude mať port 1234 otvorený
   ☐ systém, kde beží ssh klient
   ☐ `webserver`
   ☐ `sshserver`
   ☐ žiadne z predchádzajúcich

7. Katalóg bezpečnostných požiadaviek pre webové aplikácie možno nájsť v
   ☐ OWASP ASVS (Application Security Verification Standard)
   ☐ OWASP WSTG (Web Security Testing Guide)
   ☐ NIST WSS (Web Security Standard)
   ☐ NIST CF (Cybersecurity Framework)

8. V LINDDUN je sa hrozba “unawareness” týka hlavne
   ☐ procesu
   ☐ dátového toku
   ☐ dátového úložiska
   ☐ externej entity

9. Určiť, či sa konkrétna zraniteľnosť CVE-yyyy-nnnnn týka nášho systému nám pomôže k zraniteľnosti priradená informácia
   ☐ CPE (Common Platform Enumeration)
   ☐ CWE (Common Weakness Enumeration)
   ☐ CIS Benchmark
   ☐ DISA STIG (Security Technical Implementation Guide)

10. Početnosť doručených phishingových mailov používateľom čiastočne obmedzí toto technické opatrenie
    ☐ Vynucovanie silných používateľských hesiel
    ☐ Zmena mailového servera
    ☐ Skenovanie mailov
    ☐ Vzdelávanie používateľov